

ABSTRACT OF THE DISCLOSURE

According to the two party authentication method, a first party generates and transfers a random number to a second party as a first challenge. The second party
5 increments a count value in response to the first challenge, generates a first challenge response by performing a keyed cryptographic function (KCF) on the first challenge and the count value using a first key, and transfers the count value, as a second challenge, and
10 the first challenge response to the first party. The first party verifies the second party based on the first challenge, the second challenge and the first challenge response. The first party also generates a second challenge response by performing the KCF on the second
15 challenge using the first key, and transfers the second challenge response to the second party. The second party verifies the first party based on the second challenge and the second challenge response. For instance, the first and second parties can be a network and mobile, respectively, in a wireless system. Also, based on the
20 first and second challenges, both the first and second parties may generate another key.

091627767-073198